CERT

What is Microsoft EMET and why should I care?

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **22 OCT 2014**	2. REPORT TYPE **N/A**	3. DATES COVERED

4. TITLE AND SUBTITLE **What is Microsoft EMET and why should I care?**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Dormann /William**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**17**	

This material is based upon work funded and supported by DC3 under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of DC3 or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material was prepared for the exclusive use of DC3 and may not be used for any other purpose without the written consent of permission@sei.cmu.edu.

DM-0001799

ROP Mitigations

EMET 4.0 provides application-specific ROP mitigations

- LoadLibrary
- MemProt
- Caller
- SimExecFlow
- StackPivot

LoadLibrary

Extra checking when loading a library.

- e.g.don’t allow loading from a UNC path

Memprot

Check memory protection functions like VirtualProtect to make sure they are not doing things like marking stack as executable.

Caller

Before critical API functions called, disassemble backwards to verify that target function is called.

- Don’t allow return into function (“Return” of ROP)

SimExecFlow

Forward execution simulation to verify normal program execution flow.

StackPivot

When entering a critical function, make sure that stack pointer is within bounds of the stack.

EMET 5.0 New Features

EMET 5.0 includes additional exploit mitigations

- Attack Surface Reduction
- EAF+
- Deep Hooks Enabled

Attack Surface Reduction

Reducing attack surface critical to prevention of exploitation.

Examples:

- Only allow Java in Intranet IE zone.
- Don’t allow Flash in Microsoft Word

EAF

Export Address Filtering

To perform useful functionality, shellcode usually needs to call exported functions.

e.g. `kernel32!WinExec()`

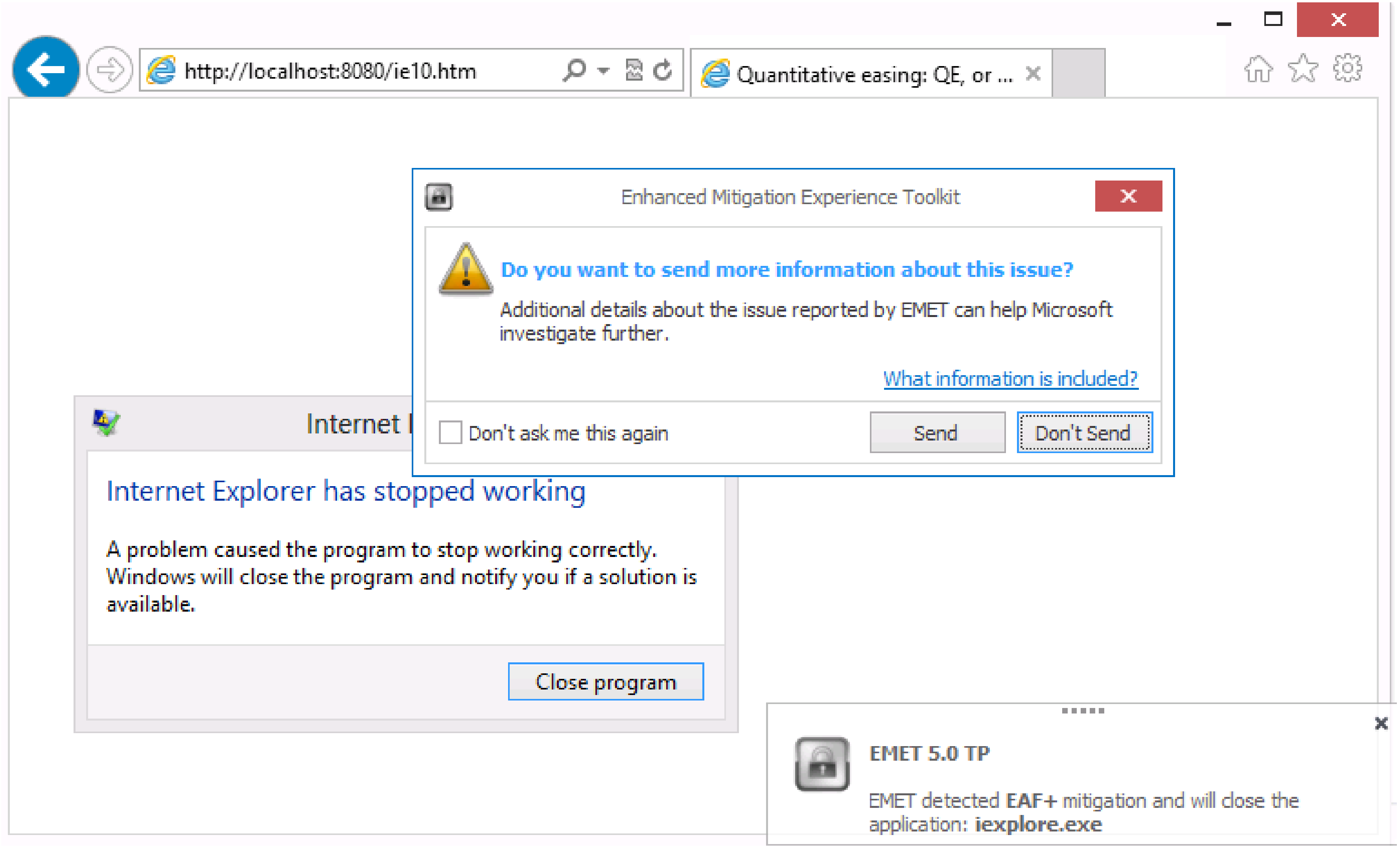
EAF blocks access to Export Address Table (EAT) based on calling address.

EAF+

Export Address Filtering +

- Added KERNELBASE export protection
- Integrity checks on stack registers and stack limits
- Prevent memory operations for export tables when they originate from suspicious modules.

EAF+ In Action



http://localhost:8080/ie10.htm
Quantitative easing: QE, or ...
Enhanced Mitigation Experience Toolkit
Internet

Do you want to send more information about this issue?

Additional details about the issue reported by EMET can help Microsoft investigate further.

What information is included?

□ Don't ask me this again

Internet Explorer has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

EMET 5.0 TP

EMET detected **EAF+** mitigation and will close the application: **iexplore.exe**

Image Credit: http://blogs.technet.com/b/srd/archive/2014/02/25/announcing-emet-5-0-technical-preview.aspx

Deep hooks

Protection of high-level functions applied towards lower-level function as well.

Microsoft has been working with vendors to make sure to ensure deep hooks compatibility.

Use EMET to stay safe

The only way to safely run applications on Windows is to use EMET!

- Minimize risk of delayed patching
- Protect against known vulnerabilities
- Protect against 0day vulnerabilities
- Protect against future vulnerabilities

EMET Recommend Configuration

System Status

DEP	**Application Opt Out**
SEHOP	**Application Opt Out**
ASLR	**Always On***

Import **`Popular Software.xml`**

Add every application you care about

* Requires Registry Change

For More Information

Visit CERT® web sites:

http://www.cert.org

http://www.cert.org/vuls/discovery/

http://www.cert.org/blogs/certcc/

Contact Presenter

Will Dormann
wd@cert.org
(412) 268-8922

Contact CERT:

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890